

FIG.1

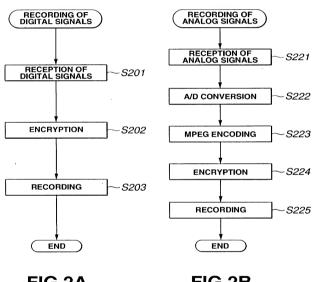


FIG.2A

FIG.2B

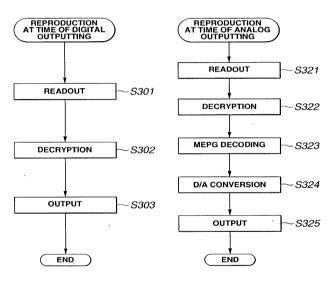
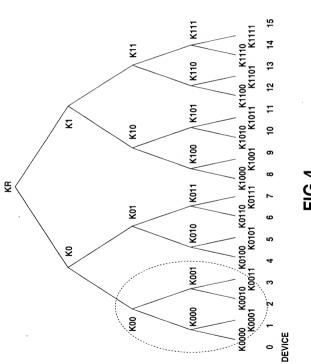


FIG.3A

Same Balle

FIG.3B



-1G.4



KRB : Key Renewal Block INSTANCE 1 SEND ROOT KEY K(t)R AT TIME t TO DEVICES 0, 1, 2

GENERATION: t				
INDEX	ENCRYPTED KEY			
0	Enc(K(t)0, K(t)R)			
00	Enc(K(t)00, K(t)0)			
000	Enc(K000, K(t)00)			
001	Enc(K(t)001, K(t)00)			
0010	Enc(K0010, K(t)001)			

FIG.5A

KRB: Key Renewal Block INSTANCE 2 SEND ROOT KEY K(t)R AT TIME t TO DEVICES 0, 1, 2

GENERATION: t				
INDEX	ENCRYPTED KEY			
000	Enc(K000, K(t)00)			
001	Enc(K(t)001, K(t)00)			
0010	Enc(K0010, K(t)001)			

FIG.5B

\$45 1 1 to

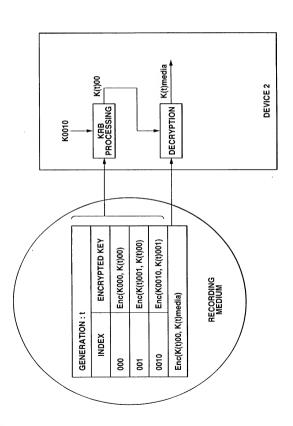


FIG.6

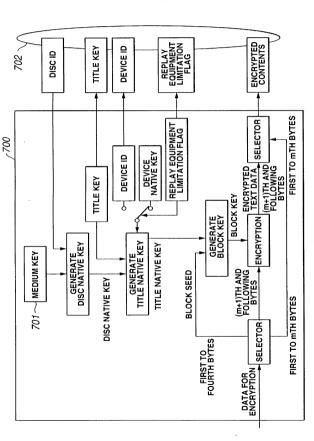


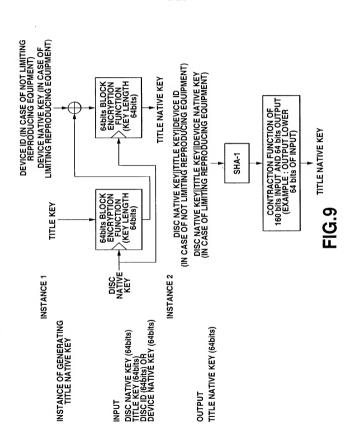
FIG.7

INSTANCE 1 INSTANCE OF GENERATING DISC NATIVE KEY DISC ID (64bits) 64bits BLOCK ENCRYPTION FUNCTION MEDIUM INPUT KEY MEDIUM KEY (64bits) (KEY LENGTH 64bits) DISC ID (64bits) DISC NATIVE KEY **INSTANCE 2** OUTPUT **DISC NATIVE KEY (64bits)** MEDIUM KEY||DISC ID SHA-1 CONTRACTION FUNCTION OF 160 bits INPUT AND 64 bits OUTPUT (EXAMPLE : OUTPUT LOWER 64bits OF INPUT)

FIG.8

DISC NATIVE KEY

. ž.



INSTANCE 1

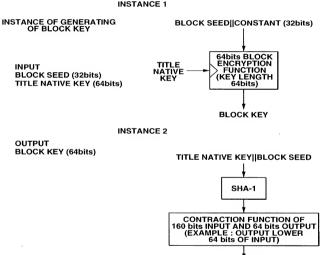


FIG.10

BLOCK KEY

11/29

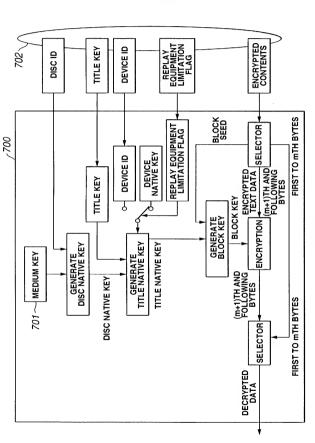
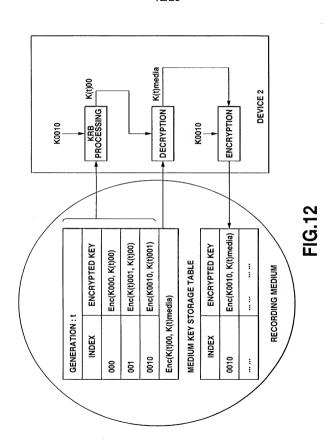


FIG.11



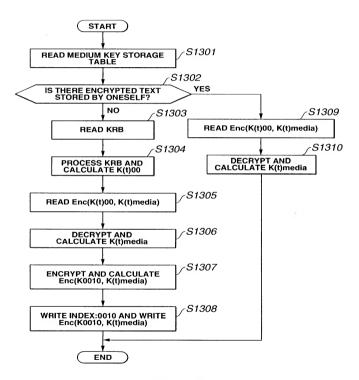


FIG.13

14/29

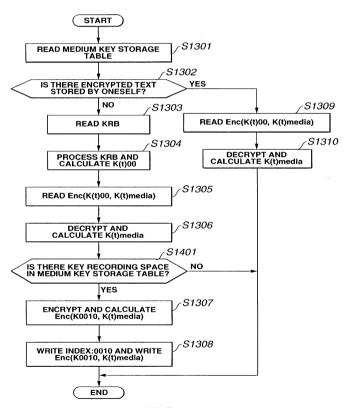
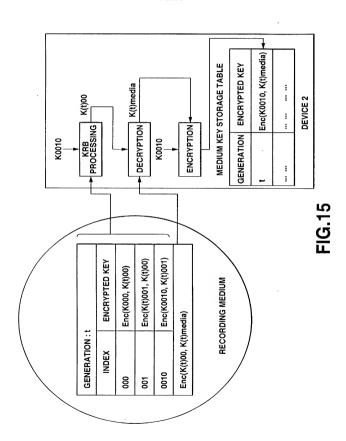


FIG.14

15/29

ोशंत **ह**ै है



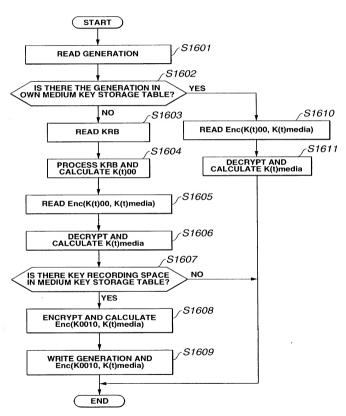
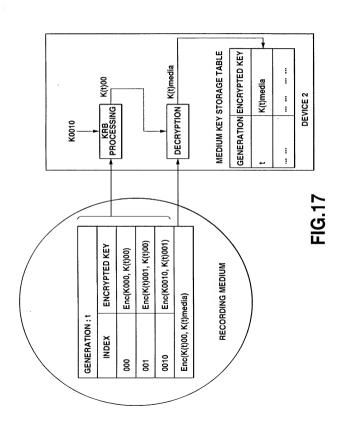


FIG.16

17/29



18/29

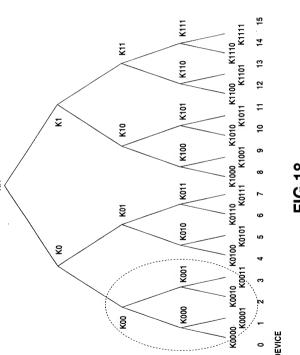


FIG.18

KRB: Key Renewal Block INSTANCE 1
SEND ROOT KEY K(t)R AT TIME t TO DEVICES 0, 1, 2

GENERATION: t				
INDEX	ENCRYPTED KEY			
0	Enc(K(t)0, K(t)R)			
00	Enc(K(t)00, K(t)0)			
000	Enc(K000, K(t)00)			
001	Enc(K(t)001, K(t)00)			
0010	Enc(K0010, K(t)001)			

FIG.19A

KRB: Key Renewal Block INSTANCE 2
SEND ROOT KEY K(t)R AT TIME t TO DEVICES 0, 1, 2

GENERATION: t				
INDEX	ENCRYPTED KEY			
000	Enc(K000, K(t)00)			
001	Enc(K(t)001, K(t)00)			
0010	Enc(K0010, K(t)001)			

FIG.19B

20/29

v	ENCRYPTED KEY	Enc(K(t)0, K(t)R)	Enc(K(t)00, K(t)0)	Enc(K000, K(t)00)	Enc(K(t)001, K(t)00)	Enc(K0010, K(t)001)	ontent)	Enc(K(s)content, content)
CONTENTS ID: s	INDEX	0	00	000	001	0010	Enc(K(t)R, K(s)content)	Enc(K(s)c
			ιτΑ					
			TION CONTENTS DATA	•				
	L	-	KEY DISTRIBUTION					

FIG.2(

Various on Gran

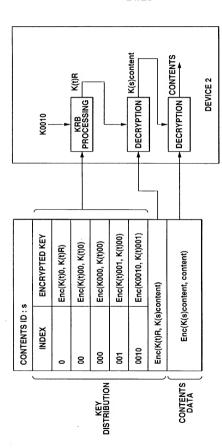


FIG.21

22/29

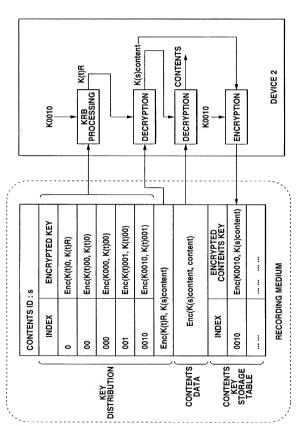


FIG.22

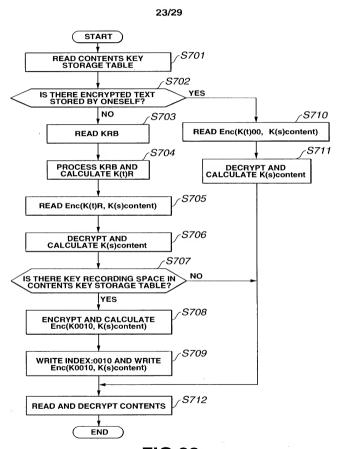


FIG.23



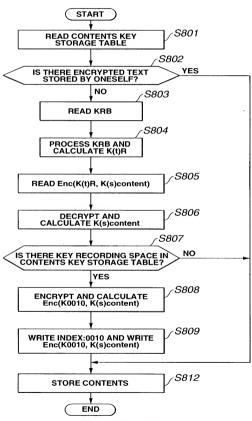
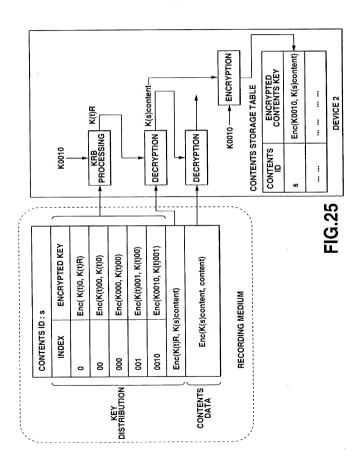


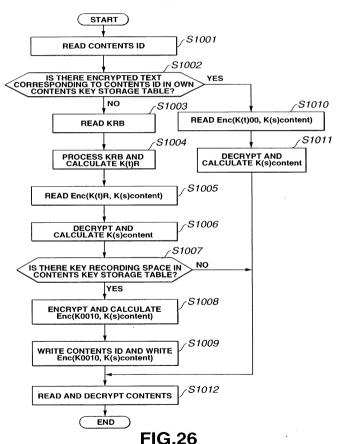
FIG.24

25/29

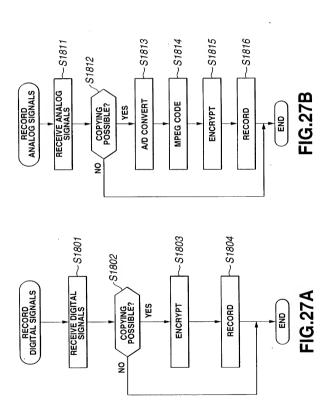
enter prim 3



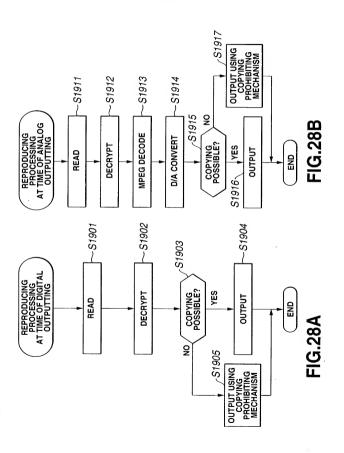




27/29



28/29



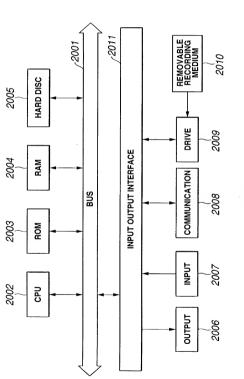


FIG.29